The Generalized Inverse of Integral Matrices

Max Koecher
Mathematics Institute
University of Münster
Münster 44, West Germany

Dedicated to Professor Helmut W. Wielandt on his seventy-fifth birthday.

Submitted by Karl Hadeler

ABSTRACT

The generalized inverse or Moore-Penrose-inverse of a real $m \times n$ matrix A is known to be the unique $n \times m$ matrix A^* satisfying the conditions (GI.1) and (GI.2) below. For a rational matrix A the generalized inverse turns out to be rational, too. Hence given an integral matrix A the description of the denominator of A^* is of interest and yields some new integral invariants of A.

1. MOTIVATION

Given a real $m \times n$ matrix A, it is well known (see [1] or [2]) that there exists a unique *generalized inverse* A^*, i.e. a real $n \times m$ matrix A^* satisfying

(GI.1) $$AA^*A = A \quad \text{and} \quad A^*AA^* = A^*,$$

(GI.2) AA^* and A^*A are symmetric.

For a rational matrix A the matrix A^* is rational, too. Hence, for integral matrices A the description of a denominator of A^* is of some interest. An explicit formula for a denominator of the generalized inverse is given in Section 6. In Section 7 the generalized inverse is applied to linear diophantine equations.

All matrices considered are real matrices. In particular,

(i) $$M^tM = 0 \quad \text{implies} \quad M = 0$$

and

52 Vanderbilt Ave., New York, NY 10017 0024-3795/85/$3.30

(ii) $\det M^tM > 0$ whenever the $m \times n$ matrix M, $m \geqslant n$, has rank n.

2. FORMULAE FOR THE GENERALIZED INVERSE

Let A denote a real $m \times n$ matrix. By the uniqueness of the generalized inverse

(i) $$(A^*)^* = A,$$

(ii) $$(A^t)^* = (A^*)^t.$$

Moreover,

(iii) $$A^* = (A^tA)^*A^t = A^t(AA^t)^*.$$

For a *proof* put $S := A^tA$ and $T := S^*S$. Hence, $A^t(AT - A) = SS^*S - S = 0$ in view of (GI.1) for S instead of A. Now $(AT - A)^t(AT - A) = (T - I)A^t(AT - A) = 0$ and $AT = A$ follows from (i) in Section 1. Hence,

$(*)$ $$A(A^tA)^*A^tA = A$$

is proved. In order to prove

$(**)$ $$AA^t(AA^t)^*A = A$$

put $R := AA^t$, $H := RR^*$, and show $(HA - A)A^t = 0$ and $(HA - A)(HA - A)^t = 0$.

Now write $B := S^*A^t$. Hence $ABA = AS^*A^tA = A$ using $(*)$, and $BAB = S^*A^tAS^*A^t = S^*A^t = B$ using (GI.1) for S instead of A. Next $AB = AS^*A^t$ becomes symmetric in view of (ii), and $BA = S^*S$ becomes symmetric in view of (GI.2) for S instead of A. Hence $B = A^*$, and the first equation of (iii) is proved. By a similar argument the second equation can be verified. ■

Note that (iii) reduces the computation of the generalized inverse of a rectangular matrix to the computation of the generalized inverse of a symmetric matrix. Moreover, $AB = 0$ implies $B^*A^* = 0$.

An immediate consequence of (iii) turns out to be

(iv) $A^* = (A^tA)^{-1}A^t$ and $A^*A = I$, whenever rank $A = n \leqslant m$,

and

(v) $A^* = A^t(AA^t)^{-1}$ and $AA^* = I$, whenever rank $A = m \leqslant n$.

3. PRIMITIVE MATRICES

An $r \times r$ matrix D is said to be in *elementary divisor normal form* if

(EN.1) D is diagonal and the diagonal elements $d_1, \ldots, d_r$ are positive integers,

(EN.2) d_{k-1} divides d_k for $2 \leqslant k \leqslant r$.

In particular, the diagonal elements $d_1, \ldots, d_r$ are the elementary divisors of D.

The appropriate tool for dealing with integral matrices is the well-known

THEOREM A. *Given* $A \in \mathrm{Mat}(m, n; \mathbb{Z})$, $A \neq 0$, *there exist* $U \in \mathrm{GL}(m; \mathbb{Z})$, $V \in \mathrm{GL}(n; \mathbb{Z})$, *and an* $r \times r$ *matrix* D, $r = \mathrm{rank}\, A$, *in elementary divisor normal form such that*

$$UAV = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}.$$

The matrix D *is uniquely determined by* A.

The integral matrix A is said to be *primitive* if A has maximal rank and if all elementary divisors of A equal 1. As a consequence of Theorem A one gets the well-known

THEOREM B. *Given* $A \in \mathrm{Mat}(m, n; \mathbb{Z})$, *where* $m > n$, *the following assertions are equivalent*:

(i) A *is primitive.*
(ii) *There exists* $B \in \mathrm{Mat}(m, m - n; \mathbb{Z})$ *such that* $(A, B) \in \mathrm{GL}(m; \mathbb{Z})$.
(iii) *There exists* $C \in \mathrm{Mat}(n, m; \mathbb{Z})$ *such that* $CA = I$.

REMARK. According to Theorem A the positive integer

$$\delta(A) := \det D \tag{iv}$$

is uniquely determined by A. Note that $\delta(A) = |\det A|$ whenever A is quadratic and $\det A \neq 0$.

4. SYMMETRIC MATRICES

Let $\mathrm{Sym}(m;\mathbb{Z})$ denote the set of symmetric integral $m \times m$ matrices. It is well known (and easy to deduce from Theorem A of Section 3) that if a nonzero matrix $S \in \mathrm{Sym}(m;\mathbb{Z})$ of rank r is given, there exist $U \in \mathrm{GL}(m;\mathbb{Z})$ and $T \in \mathrm{Sym}(r;\mathbb{Z})$ such that

$$S = U^t \begin{pmatrix} T & 0 \\ 0 & 0 \end{pmatrix} U \quad \text{and} \quad \det T \neq 0.$$

Writing

$$U = \begin{pmatrix} P \\ * \end{pmatrix}$$

there exists a *symmetric maximal rank decomposition* of S,

$$S = P^t T P \tag{i}$$

where

$$P \text{ is a primitive } r \times m \text{ matrix} \tag{ii}$$

and

$$T \in \mathrm{Sym}(r;\mathbb{Z}) \quad \text{and} \quad \det T \neq 0. \tag{iii}$$

This decomposition fails to be unique, however.

LEMMA. *Given two decompositions* $S = P_1^t T_1 P_1 = P_2^t T_2 P_2$ *satisfying* (ii) *and* (iii), *then there exists* $W \in \mathrm{GL}(r;\mathbb{Z})$ *such that* $P_1 = W P_2$ *and* $W^t T_1 W = T_2$.

Proof. Choose

$$U_j = \begin{pmatrix} P_j \\ * \end{pmatrix} \in \mathrm{GL}(m;\mathbb{Z}) \qquad \text{for} \quad j = 1,2$$

according to Theorem B of Section 3. Hence

$$U_j' \begin{pmatrix} T_j & 0 \\ 0 & 0 \end{pmatrix} U_j = S,$$

or

$$U \begin{pmatrix} T_1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} T_2 & 0 \\ 0 & 0 \end{pmatrix} V, \qquad \text{where} \quad U = \left(U_2'\right)^{-1} U_1', \quad V = U'^{-1},$$

and consequently

$$U = \begin{pmatrix} U_0 & * \\ 0 & * \end{pmatrix}, \qquad V = \begin{pmatrix} V_0 & 0 \\ * & * \end{pmatrix}$$

with

$$U_0 T_1 = T_2 V_0, \qquad V_0 = \left(U_0'\right)^{-1}.$$

Hence, $U_0, V_0 \in \mathrm{GL}(r;\mathbb{Z})$, $P_1 = (I,0)U_1 = (I,0)U'U_2 = (U_0',0)U_2 = U_0'P_2$, and $U_0 T_1 U_0' = T_2$. ∎

Given a nonzero matrix $S \in \mathrm{Sym}(m;\mathbb{Z})$ and a symmetric maximal rank decomposition $S = P'TP$, the nonzero integer

(iv) $$\omega(S) := \det T \cdot \det PP'$$

does not depend on the choice of the decomposition, according to the lemma.

REMARKS.

(a) Note that $\omega(S)$ equals $\det S$ whenever $\det S \neq 0$.

(b) Given $S \in \mathrm{Sym}(m;\mathbb{Z})$, $\operatorname{rank} S = 1$, then $\omega(S) = \operatorname{trace} S$.

(c) Let $\chi(\lambda) := \det(\lambda I - S)$ denote the characteristic polynomial of the nonzero matrix $S \in \mathrm{Sym}(m;\mathbb{Z})$, and put

$$\chi(\lambda) = \sum_{j=0}^{m} (-1)^j \omega_j(S) \lambda^{m-j}.$$

Hence $\omega(S) = \omega_r(S)$ whenever $r = \operatorname{rank} S$. In particular, $\omega(\alpha S) = \alpha^r \cdot \omega(S)$ for $0 \neq \alpha \in \mathbb{Z}$.

5. THE GENERAL MAXIMAL RANK DECOMPOSITION

Given a nonzero matrix $A \in \operatorname{Mat}(m, n; \mathbb{Z})$ of rank r, there exists a *maximal rank decomposition*

(i) $$A = PDQ$$

where

(ii) $P \in \operatorname{Mat}(m, r; \mathbb{Z})$ and $Q \in \operatorname{Mat}(r, n; \mathbb{Z})$ are primitive

and where

(iii) D is an $r \times r$ matrix in elementary divisor normal form,

according to Theorem A in Section 3. The decomposition fails to be unique; the matrix D however is uniquely determined by A.

LEMMA. *Given two maximal rank decompositions* $A = P_1 D Q_1 = P_2 D Q_2$, *there exists* $W \in \operatorname{GL}(r; \mathbb{Z})$ *such that*

$$W' := D^{-1} W D \in \operatorname{GL}(r; \mathbb{Z}) \quad \textit{and} \quad P_1 = P_2 W,\ Q_1 = W'^{-1} Q_2.$$

Proof. Choose

$$U_j = (P_j, *) \in \operatorname{GL}(m; \mathbb{Z}), \quad V_j = \begin{pmatrix} Q_j \\ * \end{pmatrix} \in \operatorname{GL}(n; \mathbb{Z}) \qquad \text{for} \quad j = 1, 2$$

according to Theorem B in Section 3. Hence,

$$U \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} V, \qquad \text{where} \quad U := U_2^{-1} U_1, \quad V := V_2 V_1^{-1},$$

and therefore

$$U = \begin{pmatrix} U_0 & * \\ 0 & * \end{pmatrix}, \quad V = \begin{pmatrix} V_0 & 0 \\ * & * \end{pmatrix} \qquad \text{with} \quad U_0 D = D V_0$$

where $U_0, V_0 \in \mathrm{GL}(r;\mathbb{Z})$. Now

$$P_1 = U_1\begin{pmatrix} I \\ 0 \end{pmatrix} = U_2\begin{pmatrix} U_0 \\ 0 \end{pmatrix} = P_2U_0,$$

$$Q_1 = (I,0)V_1 = \left(V_0^{-1},0\right)V_2 = V_0^{-1}Q_2. \qquad \blacksquare$$

Given a nonzero matrix $A \in \mathrm{Mat}(m,n;\mathbb{Z})$ and a maximal rank decomposition $A = PDQ$, the positive integer

(iv) $$\nu(A) := \det P^tAQ^t = \det D \cdot \det P^tP \cdot \det QQ^t$$

does not depend on the choice of the maximal rank decomposition according to the lemma. In particular,

(v) $\nu(\alpha A) = |\alpha|^r \cdot \nu(A)$ whenever $0 \neq \alpha \in \mathbb{Z}$ and $r = \operatorname{rank} A$,

(vi) $$\nu(A^t) = \nu(A),$$

(vii) $\nu(A) = |\det A|$ whenever A is quadratic and $\det A \neq 0$,

(viii) $\nu(P) = \det P^tP$ whenever $P \in \mathrm{Mat}(m,r;\mathbb{Z})$, $m \geqslant r$, is primitive,

(ix) $\nu(A) = \nu(P)\cdot\nu(D)\cdot\nu(Q)$ whenever $A = PDQ$ is a maximal rank decomposition.

In view of (iv) in Section 4, the integers $\omega(A^tA)$ and $\omega(AA^t)$ are defined for a nonzero matrix $A \in \mathrm{Mat}(m,n;\mathbb{Z})$.

THEOREM. *Given a nonzero matrix* $A \in \mathrm{Mat}(m,n;\mathbb{Z})$, *then*

$$\omega(A^tA) = \omega(AA^t) = \nu(A)\cdot\delta(A).$$

Proof. Choose a maximal rank decomposition $A = PDQ$. Hence,

$$A^tA = Q^tTQ, \qquad \text{where} \quad T := DP^tPD,$$

turns out to be a symmetric maximal rank decomposition according to (ii) in

Section 1. Hence, (iv) in Section 4 yields

$$\begin{aligned}\omega(A^tA) &= \det T \cdot \det QQ^t = (\det D)^2 \cdot \det P^tP \cdot \det QQ^t \\ &= \nu(A)\cdot\delta(A)\end{aligned}$$

according to (iv) above and (iv) in Section 3.

The proof is complete because the right side of the equation turns out to be invariant under the transposed mapping. ■

There is another description of $\omega(A^tA)$ using subdeterminants of A:

PROPOSITION. *Given a nonzero matrix* $A \in \mathrm{Mat}(m, n; \mathbb{Z})$ *of rank* r, *then* $\omega(A^tA)$ *equals the sum of the squares of all* $r \times r$ *subdeterminants of* A.

Proof. In order to see that the assertion is invariant under the mappings $A \mapsto UAV$, where U and V are orthogonal, use Remark (c) in Section 4 and consider the generators of the orthogonal matrices that are built up by 2×2 orthogonal matrices. Then choose orthogonal matrices U and V such that

$$A = U\begin{pmatrix} T & 0 \\ 0 & 0 \end{pmatrix}V, \qquad \text{where } T \text{ is diagonal.}$$

Hence both sides of the assertion equal $(\det T)^2$. ■

REMARK. There exists an amusing identity for the numbers $\nu(A)$: Given nonzero integral matrices A, B, and C such that the product ABC is defined and such that

$$\operatorname{rank} ABC = \operatorname{rank} A = \operatorname{rank} B = \operatorname{rank} C,$$

then

$$\nu(ABC)\cdot\nu(B) = \nu(AB)\cdot\nu(BC).$$

6. THE GENERALIZED INVERSE

Let

(i) $$A = PDQ$$

be a maximal rank decomposition of the nonzero matrix $A \in \mathrm{Mat}(m, n; \mathbb{Z})$.

From (iv) and (v) in Section 2 one gets

(ii) $$P^* = (P^tP)^{-1} \quad \text{and} \quad P^*P = I$$

as well as

(iii) $$Q^* = Q^t(QQ^t)^{-1} \quad \text{and} \quad QQ^* = I.$$

Hence by the uniqueness of the generalized inverse a verification yields

THEOREM. *Given a maximal rank decomposition* $A = PQD$, *then*

(iv) $$A^* = Q^tG^{-1}P^t, \qquad \textit{where} \quad G = P^tAQ^t = P^tP \cdot D \cdot QQ^t.$$

COROLLARY 1. $A^*A = Q^t(QQ^t)^{-1}Q$ *and* $AA^* = P(P^tP)^{-1}P^t$.

COROLLARY 2. $A^* = (PDQ)^* = Q^*D^{-1}P^*$.

COROLLARY 3. $\nu(A) \cdot A^*$ *is integral, and the rational matrix* $[1/\nu(A)]A$ *has an integral generalized inverse.*

In particular, $\nu(A)$ turns out to be a denominator of A^*, and numerical examples show that $\nu(A)$ in general is best possible.

Choosing $U \in \mathrm{GL}(m;\mathbb{Z})$ and $D \in \mathrm{Mat}(r;\mathbb{Z})$, $r = \operatorname{rank} A$, in elementary divisor normal form such that

(v) $$A = U\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}V, \qquad U = (P, *), \quad V = \begin{pmatrix} Q \\ * \end{pmatrix},$$

then $A = PDQ$ becomes a maximal rank decomposition. Writing

(vi) $$U^tU = \begin{pmatrix} S & X \\ X^t & * \end{pmatrix},$$

where S is $r \times r$ integral symmetric and $\det S \neq 0$,

(vii) $$VV^t = \begin{pmatrix} T & Y^t \\ Y & * \end{pmatrix}$$

where T is $r \times r$ integral symmetric and $\det T \neq 0$, and using $S = P'P$, $T = QQ'$, $G = SDT$, the generalized inverse A^* of A according to (iv) becomes

(viii)
$$A^* = V' \begin{pmatrix} T^{-1}D^{-1}S^{-1} & 0 \\ 0 & 0 \end{pmatrix} U'$$
$$= V \begin{pmatrix} D^{-1} & D^{-1}S^{-1}X \\ YT^{-1}D^{-1} & YT^{-1}D^{-1}S^{-1}X \end{pmatrix} U^{-1}.$$

In particular,

(ix)
$$AA^* = U \begin{pmatrix} I & S^{-1}X \\ 0 & 0 \end{pmatrix} U^{-1}, \qquad A^*A = V^{-1} \begin{pmatrix} I & 0 \\ YT^{-1} & 0 \end{pmatrix} V.$$

REMARK. The question under which circumstances the generalized inverse of an integral matrix A becomes integral can be answered: Given a nonzero matrix $A \in \mathrm{Mat}(m, n; \mathbb{Z})$ of rank n, then the following assertions are equivalent:

(a) A^* is integral,
(b) AA^* is integral,
(c) $A'A \in \mathrm{GL}(n; \mathbb{Z})$,
(d) $A = P \begin{pmatrix} B \\ 0 \end{pmatrix}$, where $B \in \mathrm{GL}(n; \mathbb{Z})$ and where $P \in \mathrm{GL}(n; \mathbb{Z})$ is orthogonal.

7. THEOREM ON DIOPHANTINE EQUATIONS

THEOREM. *Given a nonzero matrix* $A \in \mathrm{Mat}(m, n; \mathbb{Z})$ *and* $b \in \mathbb{Z}^m$, *the following assertions are equivalent*:

(i) *There exists an integral solution* x *of the diophantine equation* $Ax = b$.

(ii) (1) $AA^*b = b$,

(2) $g'A^*b \in \mathbb{Z}$ *for all* $g \in \mathbb{Z}^n$ *such that* $A^*Ag = g$.

Proof. In the notation of (v) in Section 6, put

$$y = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = Vx, \qquad c = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = U^{-1}b.$$

Then (i) becomes equivalent to

(i*) $\qquad c_2 = 0 \quad \text{and} \quad D^{-1}c_1 \text{ is integral.}$

In this case the general integral solution is given by

(*) $\qquad y = \begin{pmatrix} D^{-1}c_1 \\ p \end{pmatrix}, \qquad \text{where} \quad p \in \mathbb{Z}^{n-r} \text{ is arbitrary.}$

Using (ix) in Section 6, condition (ii) (1) has the same meaning as

$$\begin{pmatrix} I & * \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix},$$

and hence as

(ii*) (1) $\qquad c_2 = 0.$

Next consider $g \in \mathbb{Z}^n$ such that

(1) $\qquad A^*Ag = g.$

Putting

(2) $\qquad h := V^{t-1}g = \begin{pmatrix} h_1 \\ h_2 \end{pmatrix} \in \mathbb{Z}^n,$

then (1) is equivalent to $V^{t-1}A^*AV^th = h$, and hence to $(VA^*AV^{-1})'h = h$, using (GI.2). So by (ix) in Section 6, condition (1) can be stated as

$$\begin{pmatrix} I & * \\ 0 & 0 \end{pmatrix}\begin{pmatrix} h_1 \\ h_2 \end{pmatrix} = \begin{pmatrix} h_1 \\ h_2 \end{pmatrix},$$

i.e. as

(3) $\qquad h = \begin{pmatrix} h_1 \\ 0 \end{pmatrix}, \qquad h_1 \in \mathbb{Z}^r \text{ arbitrary.}$

Under condition (ii*) (1) one calculates

$$g^t A^* b = h^t \begin{pmatrix} D^{-1} & * \\ * & * \end{pmatrix} c = h_1^t D^{-1} c_1,$$

using (viii) in Section 6, and (2) and (3) above. Hence $g^t A^* b$ is integral for all $g \in \mathbb{Z}^n$ satisfying (1) if and only if $D^{-1}c_1$ is integral. In view of (ii*) (1), the conditions (i) and (ii) turn out to be equivalent. ■

REMARKS.

(a) Note that (ii) (1) is equivalent to the solvability of $Ax = b$ over $\mathbb{Q}$. Hence, it is well known that the general *rational* solution of $Ax = b$ is given by $x = z - A^*Az + A^*b$, where $z \in \mathbb{Q}^n$.

(b) The rational solutions of $A^*Ag = g$ are of course given by $g = A^*Ar$, $r \in \mathbb{Q}^m$, because A^*A is idempotent. Hence, (ii) may be replaced by

(iii) (1) $AA^*b = b$,

(2) $r^t A^* b \in \mathbb{Z}$ for all $r \in \mathbb{Q}^m$ such that $A^*Ar \in \mathbb{Z}^n$.

My thanks are due to Dr. Krieg for his careful reading of the manuscript.

REFERENCES

1 A. Ben-Israel and Th. N. E. Greville, *Generalized Inverses*, Wiley, New York, 1974.

2 S. L. Campbell and C. D. Meyer, Jr., *Generalized Inverses of Linear Transformations*, Pitman, London, 1979.

Received 28 August 1984; revised 14 June 1985